

UNITED STATES DISTRICT COURT

for the
Western District of Arkansas

US DISTRICT COURT
WESTERN DIST ARKANSAS
FILED

OCT 10 2018

DOUGLAS F. YOUNG, Clerk
By Deputy Clerk

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
14431 Gains Road
Fayetteville, Arkansas 72701

Case No. FA 18-96

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Western District of Arkansas (identify the person or describe property to be searched and give its location): See "Attachment A"

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized): See "Attachment B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of 18 U.S.C. § 2252/2252A, and the application is based on these facts: See "Attachment C"

☒ Continued on the attached sheet.

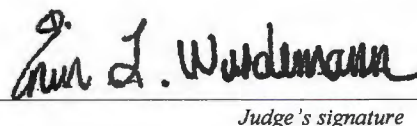
☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

William DeVito, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 10/10/18


Judge's signature

City and state: Fayetteville, Arkansas

ERIN L. WIEDEMANN, U.S. MAGISTRATE JUDGE
Printed name and title

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

Any and all structures and outbuildings to include vehicles located on the property or arriving on the property and curtilage of **14431 Gains Road, Fayetteville, Arkansas 72701** (the "SUBJECT PREMISES"), more particularly described as a single-story residential home with a grey colored metal roof and yellow siding. The residence is located on the west side of Gaines Road and the front door faces east.

ATTACHMENT B
ITEMS TO BE SEARCHED FOR AND SEIZED

- a. Images of child pornography, including any and all digital images stored on devices capable of such, and files containing images of child pornography in any form wherever it may be stored or found including, but not limited to:
- i. any and all computer hardware and software capable of storing, accessing, sending or receiving digital information, computer system, computer tablet, smart phones, micro SD cards, and related peripherals, or any other device capable of accessing the internet and/or storing digital data; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, internal or external storage devices, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to cellular telephones, hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Blue Ray players, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;
 - ii. any and all applications (apps) contained on any electronic device, books and magazines, digital or otherwise, containing visual depictions of minors engaged in sexually explicit conduct or involving the physical description of sexual activity involving minors
 - iii. originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
 - iv. motion pictures, films, videos, film negatives, digital or print copies, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

b. information or correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, that were transmitted or received using computer or any internet capable device, or any other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- i. envelopes, letters, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and
- ii. books, records, and any other written or digital information bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

c. Any and all credit card information including but not limited to bills and payment records for subscription to internet or non internet based companies allowing access to images of minors engaging in sexually explicit activities, or reflecting the purchase of or access to any material related to child pornography ;

d. Any and all correspondence pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 whether transmitted or received using computer, a facility or means of interstate commerce, common carrier, or mail.

e. Any and all computer-related documentation to include written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items. In addition to passwords, to include alphanumeric strings, pass-phrases, password files, and similar decryption codes necessary to access data that is encrypted or otherwise inaccessible.

f. Any and all security devices, to include physical keys, encryption devices, "dongles", and similar physical items needed to gain access to associated computer hardware. In addition, peripherals, equipment that send data to, or receive data from, computer hardware, but do not normally store user data, such as keyboards, mice, printers, scanners, plotters, video display monitors, modems, cables, and certain types of facsimile machines.

g. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256.

h. Any and all diaries, notebooks, notes and any other electronic records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, and Section 2256.

k. In searching the data, the computer personnel may copy all of the data contained in the computer equipment and storage devices. In doing so, the search is authorized to allow the computer personnel to recover and examine: all images contained upon any seized device wherever they may be found, a search of unallocated spaces for images related to child pornography, a search to identify Peer-to-Peer programs, a search of terms related to child pornography, and any other search and examination that would reveal the existence of child pornography on the seized item including deleted, hidden, accessing applications (apps), and/or encrypted data. Emails, data files, and any other electronic information related to the ownership of the seized electronic media may be copied, imaged and examined during purposes of conducting the forensic examination.

ATTACHMENT C
UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF ARKANSAS

STATE OF ARKANSAS

:
:
:
:

ss. JIMMY LEE HALL

COUNTY OF WASHINGTON

Affidavit in Support of Application for Search Warrant

I, William DeVito, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”), currently assigned to the Assistant Special Agent in Charge Office in Fayetteville, Arkansas. I have been so employed with HSI since July, 2011. As part of my daily duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, online enticement, transportation, receipt and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2251A, 2422(b), 2252(a) and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have also participated in the execution of numerous search warrants and arrest warrants, a number of which involved child exploitation and/or child pornography

offenses. This affidavit is being submitted based on information from my own investigative efforts as well as information obtained from others who have investigated this matter and/or have personal knowledge of the facts herein.

2. This affidavit is being submitted in support of an application for a search warrant for the premises located at **14431 Gains Road, Fayetteville, Arkansas 72701** the “SUBJECT PREMISES”. As such, it does not include all of the information known to me as part of this investigation, but only information sufficient to establish probable cause for the requested search warrant.

Statutory Authority

3. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors, which has been defined in Title 18 U.S.C. 2256, as an individual under 18 years of age.

a. Under 18 U.S.C. Section 2252(a)(1) (transportation), 2252(a)(2) (receipt and distribution), and 2252(a)(4)(B) and 2252A(a)(5)(B) (possession), it is a federal crime for any person to transport, distribute, receive, and possess child pornography, as that term is defined by federal law. Further under 18 U.S.C. Section 2253(a)(3), a person who is convicted of an offense under 18 U.S.C. Section 2252 or 2252A, shall forfeit to the United States such person’s interest in any property, real or personal, used or intended to be used to commit or to promote the commission of such offense.

Computers and Child Pornography

4. Based upon my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement

officers with whom I have had discussions, I know that computers and computer technology have revolutionized the way in which child pornography is produced, distributed and utilized. Prior to the advent of computers and the Internet, child pornography was produced using cameras and film, resulting in either still photographs or movies. The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce the images. As a result, there were definable costs involved with the production of pornographic images. To distribute these images on any scale also required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent exposure to the public. The distribution of these wares was accomplished through a combination of personal contacts, mailings, and telephone calls, and compensation for these wares would follow the same paths. More recently, through the use of computers and the Internet, distributors of child pornography use membership-base/subscription-based websites to conduct business, allowing them to remain relatively anonymous.

5. In addition, based upon my own knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which those who seek out child pornography are able to obtain this material. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by those who seek to obtain access to child pornography in these ways:

6. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer-readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

7. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial Internet Service Providers (ISPs), such as America Online ("AOL") and Microsoft, which allow subscribers to dial a local number and connect to a network which is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet or the World Wide Web.

8. The Internet allows users, while still maintaining anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) websites that offer images

of child pornography. Those who seek to obtain images or videos of child pornography can use standard Internet connections, such as those provided by business, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions involving those who wish to gain access to child pornography over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the websites and images accessed by the recipient.

9. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a "hard drive") used in home computers has grown tremendously with the last several years. Hard drives with the capacity of 160 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime." Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

10. It should be noted that Internet Protocol (IP) numbers are unique identifiers leased to internet customers by their ISP's. Although IP numbers are capable of changing over time, only one (1) unique IP number can be assigned to a given customer's computer at any given time. Logs of these leased IP's (and their assigned customer accounts) are stored by ISP's routinely.

11. Your Affiant knows from his own experience and the training and experience of other law enforcement officers that Internet computers identify each other by an Internet Protocol or IP address. These IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can typically lead the law enforcement officer to a particular Internet service company and that company can typically identify the account that uses the address to access the Internet.

Background Regarding Gmail Accounts

12. Based on my knowledge and experience and information obtained from other law enforcement personnel with training and experience in this area, the following is known about Gmail accounts:

- a. Gmail is a free, advertising supported email service provided by Google. Users may access Gmail as secure webmail.
- b. Gmail initially started as an invitation-only beta release on April 1, 2004 and it became available to the public on February 7, 2007.
- c. Individual Gmail messages, including attachments, may be up-to 25 MB. Gmail has a search-oriented interface and a "conversation view" similar to an Internet Forum.

- d. Users can buy additional storage, shared among Gmail, Google Drive and Google+ Photos, through a monthly subscription plan. As of 2015, storage up to 15 GB is free, and paid plans are available for up to 30 TB for personal use.
- e. Google updated the Gmail inbox with tabs which allow the application to categorize the user's emails. The five tabs are: Primary, Social, Promotions, Updates and Forums. These tabs also appear in Gmail's mobile version.
- f. Gmail Mobile is a free service developed to provide access to Gmail from mobile devices. Gmail Mobile offers many of the features as Gmail delivered effectively to smaller, mobile screens.
- g. In 2010, Google commenced its new social networking tool, Google Buzz, which integrated with Gmail allowing users to share links and media, as well as status updates with social media platforms.

PROBABLE CAUSE

9. On August 1, 2018, your Affiant received Cyber Tip Line Report Numbers 35774198 and 37143827 from the National Center for Missing and Exploited Children (NCMEC) in reference to media files containing what was believed to be child pornography being uploaded onto the Google Photos infrastructure.

10. The information on the suspected media containing child pornography was submitted to the Cyber Tip Line by Google on July 3, 2018 and July 24, 2018, respectively. The incident information was categorized as being "Apparent Child Pornography" which was identified by Google representatives on all uploaded images and videos. A total of

approximately three (3) uploaded files of suspected child pornography were linked to the reports. Two of said image files were identified as “viewed” by Google representatives prior to submission.

11. Google provided the Cyber Tip Line 35774198 with the following information of the user being reported:

Incident Type: Child Pornography (possession, manufacture, and distribution)

Name/User: Jimmy Hall

Phone: 4792495059

Email Address: JimmyHall1958@gmail.com

IP Address: 72.204.52.120

Number of Uploaded Files: 1

12. Your Affiant viewed the file linked to the Cyber Tip Line Report and determined it to in fact be an image of child pornography. On October 1, 2018, your Affiant again viewed and described one (1) of these files as follows:

(a) File Name: 457B51DC-E3A2-4D30-9F39-59E48A24D5A5-223-0000002C1E3B2252.JPEG

This image depicts what is believed to be a four (4) to six (6) year old minor female laying on a bed with her legs spread and her skirt up; touching a penis. The face of the minor female is visible.

13. Google provided the Cyber Tip Line 37143827 with the following information of the user being reported:

Incident Type: Child Pornography (possession, manufacture, and distribution)

Name/User: James Wall

Phone: 4792495059

Email Address: jimmyhall099@gmail.com

IP Address: 2600:8804:8442:9d00:5dd6:ccfd:45f4:a481

Number of Uploaded Files: 2

14. Your Affiant viewed the files linked to the Cyber Tip Line Report 37143827 and determined them to in fact be child pornography; these files are in Graphics Interchange Format, more commonly known as GIF's; GIF's are short, moving images that resemble a video clip. On October 1, 2018, your Affiant again viewed and described two (2) of these files as follows:

- (a) File Name: 5E2E12B5-6B8C-49CD-80C3-26244D0211FD-1156-000000DBB47C4C00.GIF

This GIF is approximately seven (7) seconds long and depicts what is believed to be a four (4) to six (6) year old minor female laying on a bed with her legs spread being anally penetrated by a penis.

- (b) File Name: 6E7CCF26-9C01-42F7-8FB6-EE71325FC5A5-1156-000000DA1A7AD54F.GIF

This GIF is approximately seven (7) seconds long and depicts what is believed to be a six (6) to eight (8) year old minor female laying down and being orally penetrated by a penis.

15. An internet search on the origins of IP addresses 2600:8804:8442:9d00:5dd6:ccfd:45f4:a481 and 72.204.52.120 found them to be issued to the internet service provider Cox Communications. Documents received on or about September 13, 2018, from Cox Communications in reference to IP addresses 2600:8804:8442:9d00:5dd6:ccfd:45f4:a481 and 72.204.52.120 identified the IP's as being assigned to Tamara STEVENS at 14431 Gains Road, Fayetteville, Arkansas 72701, the SUBJECT PREMISES, during the relevant time period.

16. Your Affiant conducted Department of Homeland Security (DHS), law enforcement, and open source database queries on the SUBJECT PREMISES which indicated,

that as of July 2018, Jimmy HALL, with a date of birth in 1991, currently resides at the residence. HALL also has a phone number listing of 479-249-5059, which is the same phone number provided in the account information linked to the Cyber Tip Line Reports 35774198 and 37143827. HALL has also provided this phone number as well as the SUBJECT PREMISES to law enforcement as his contact information. Law enforcement queries as well as publicly accessible social media revealed Jimmy HALL is married to Johnelle HALL; Johnelle HALL's maiden name is STEVENS. Further database queries revealed Johnelle HALL and Tamara STEVENS are related.

17. Your Affiant conducted surveillance of the SUBJECT PREMISES and located a 2001 Dodge pickup registered to Johnelle HALL and an older model Chevrolet Blazer K-10. The license plate of the Chevrolet was not visible but records checks revealed a 1979 Chevrolet Blazer K-10 was assessed in 2017 by Jimmy HALL of 14431 Gains Road, Fayetteville, Arkansas 72701. Additionally, the mailboxes for the neighborhood are collocated near the main road and the mailbox for house number 14431 has the name HALL marked on its exterior. Surveillance also revealed two (2) WiFi signals in proximity of the SUBJECT PREMISES, both of which were secure networks.

Conclusion

20. *Necessity of On-site and Off-site examinations of entire computers or storage media.* Based on my experience and the training and experience of other agents, many of the items sought in this affidavit may be stored electronically. Based on my experience and consultation with computer forensic experts, I know that electronic files can be easily moved from computer or electronic storage medium to another computer or medium. Therefore,

electronic files downloaded to or created on one computer can be copied on or transferred to any other computer or storage medium at the same location. In addition, based on my experience, I know that searching computerized information for evidence of crime often requires special agents to seize most or all of a computer system's central processing unit (CPU), input/output peripheral devices, related software, documentation, and data security devices, including passwords, so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

(a) Volume of evidence: Computer storage devices such as hard disks, diskettes,

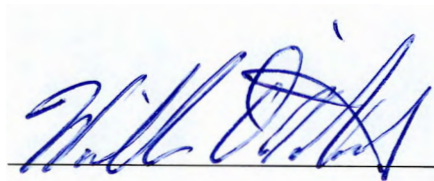
tapes and laser disks, can store the equivalent of thousands of pages of information. This sorting process can take up to several months to complete, depending on the volume of data stored. Therefore, it would also be impractical to attempt this type of data search on site.

(b) Technical requirements: Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional destruction (both from external sources and from destructive code embedded in the system such as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

21. Therefore, authorization is sought in this application to seize the items set forth in attachment "B" that are found on the premises to be searched, in order to examine those items for evidence. If it is determined that data has been seized that does not constitute evidence of the crimes detailed herein, the government will return said data within a reasonable time.

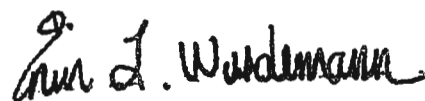
22. Based on my experience and the training and experience of other agents involved with this investigation, your affiant knows that individuals involved in the sexual exploitation of children through child pornography almost always keep copies of their sexual explicit material. Among the reasons copies are maintained is because child pornography is illegal to openly purchase, and the most common method of acquiring it is by trading with other people with similar interests. It is also known that due to the inherent illegality of these sexually explicit materials, they are most often kept in a place considered secure, usually a residence, to avoid detection by law enforcement.

23. Based on the foregoing information, probable cause exists to believe there is located at **14431 Gains Road, Fayetteville, Arkansas 72701**, the SUBJECT PREMISES, evidence of violations of Title 18, United States Code, Section 2252, et seq. Your Affiant prays upon his honorable court to issue a search warrant for the SUBJECT PREMISES for the items set forth in attachment "B" (which is attached hereto and incorporated herein by reference), that constitute evidence, fruits, and instrumentalities of violation of Title 18, United States Code, Section 2252, et seq.



William DeVito, Special Agent
Homeland Security Investigations

Affidavit subscribed and sworn to before me this 10th day of October 2018.



Erin L. Wiedemann
United States Magistrate Judge